
Protect Your Data
the Way Banks
Protect Your Money
ca
technologies

A New Security Model Worth Understanding—and Emulating

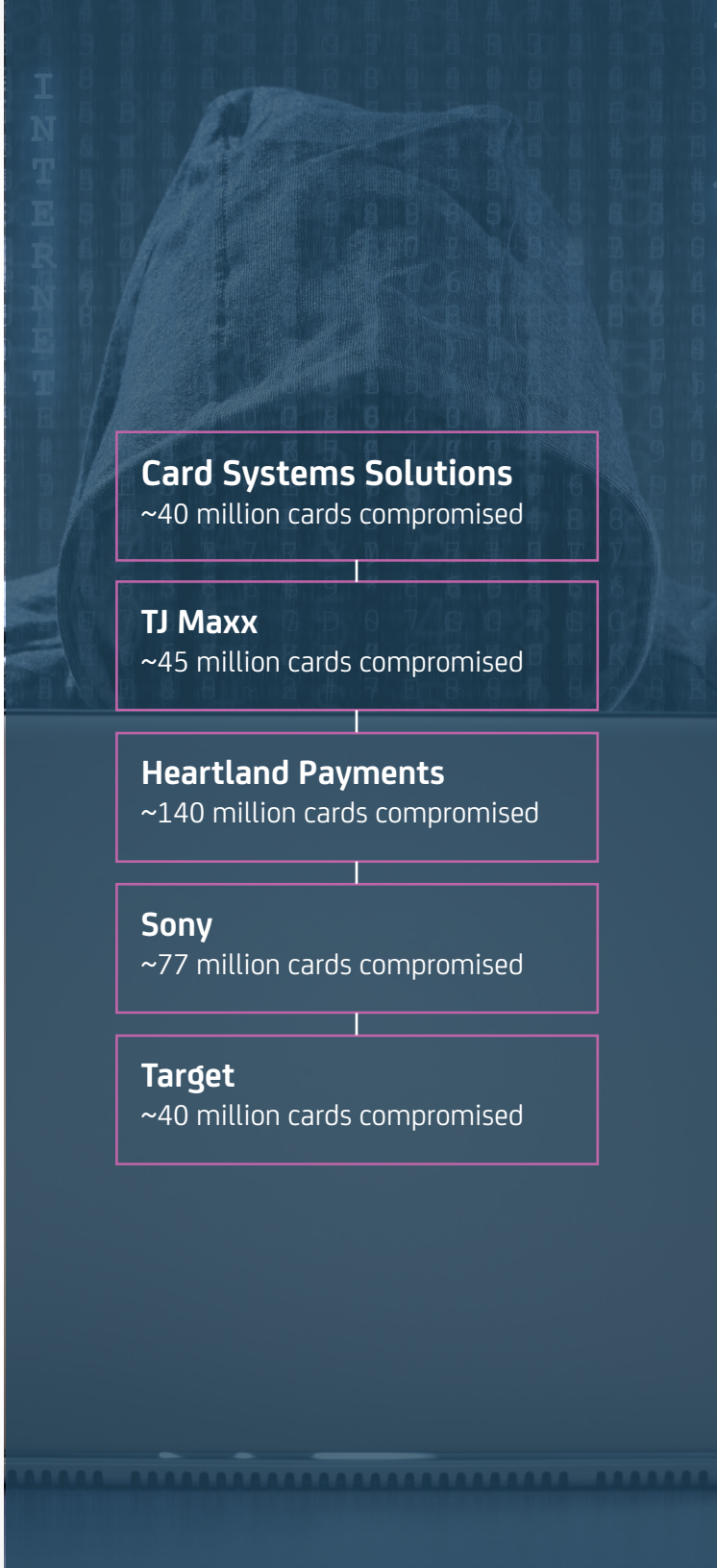
Enterprise security traditionally relied on a fortress strategy that locked down user endpoints and created walls around the network. Today, this strategy cannot support or secure the use of mobile devices and SaaS capabilities, which exist outside the fortress. As a result, Chief Information Security Officers (CISOs) have been looking for new solutions that can secure these technologies today, and adapt as threats and business needs change.

The credit card industry's security model is one example that provides a new way to think about risk and contain it—that is, if you can see past the occasional bad rap it's gotten from attacks and breaches.

While credit card data breaches are often big news stories, they haven't severely damaged the industry. In fact, they've shown that while fraud remains a persistent global threat, it's also a consistently manageable one. The resilience of credit cards is exactly why their security model is worth understanding—and emulating.

For example, Target's much-discussed security breach caused significant pain for the company and its customers. Yet, overall use of credit and debit cards did not decline. According to the 2016 Federal Reserve Payments Study, the number of credit card payments reached 33.8 billion in 2015 with a value of $3.16 trillion, up 6.9 billion or $0.61 trillion since 2012.[1] Consumers may have shopped less at Target stores for a time, but they were using payment cards and electronic payments more than ever.

More important, despite repeated and significant compromises of credit card data over the past two decades, payment card fraud has been held at a tolerable level.



1 Federal Reserve System, "The Federal Reserve Payments Study 2016," December, 2016.

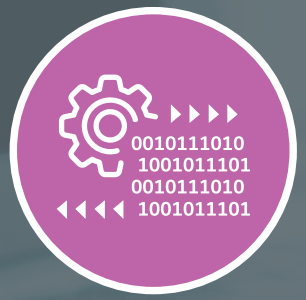
The Credit Card Security Model

The security model deployed by credit and debit card systems is significantly different than traditional corporate data security solutions. Understanding the critical differences between credit card security and traditional IT security is important.

You may think the difference is Payment Card Industry (PCI) standards, which mandate a variety of traditional IT security controls and processes for anyone processing payment card data. These standards are important and laudable, but in general, they're primarily best practices. PCI is not what makes payment card security special.

The following systemic characteristics represent the true differentiators that have enabled credit and debit card security to mitigate fraudulent transactions over time:

Live monitoring and real-time control



Data-driven

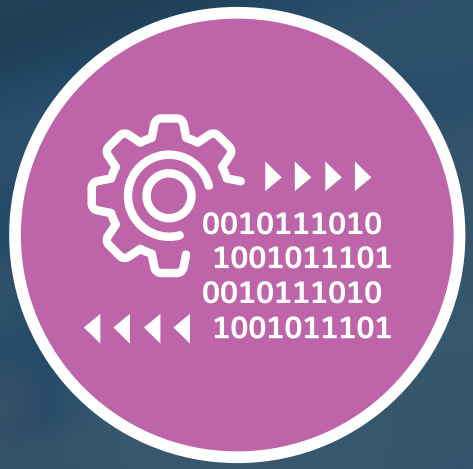
Integrated controls that are endpoint-independent

Live Monitoring and Real-Time Control

The payment card security system does not rely exclusively on the integrity of individual cards, networks or endpoints to ensure security—but rather on real-time monitoring and authorization of transactions.

Every time someone swipes a credit or debit card, an authorization request is sent in real time to the issuing bank. That authorization request notifies the bank of the transaction and asks for its approval—which the bank must provide before the transaction will be allowed. This provides the bank with the visibility needed to monitor live activities and the ability to enforce real-time controls on every action initiated by a card. If a transaction is considered risky, the bank has the option to monitor the card transactions more closely, request additional information by contacting the cardholder or to deny the transaction.

Data-Driven



Payment card security is data-driven and manages risk over time. Because the card-issuing bank sees all of a cardholder's purchases, it's able to analyze the activity of individual users and cards over time. The insights gained from analytics are used to control access to the resource being protected: money.

The bank authorizes or denies each transaction in real time based not only on the details of the transaction being authorized but on insight provided by integrated analytics, including:

- Behavior analytics that recognize inconsistencies with past activities.
- Similarities with known malicious activities.
- Insight regarding user trends and activities.
- Risk assessment of the activity based on all available information.

By using data and analytics, the bank's payment card security system is able to adapt and evolve as threats, risks and business needs change over time.

Integrated Controls That Are Endpoint-Independent

The payment card security model leverages risk controls that are integrated into their system but are largely endpoint-independent. These controls provide a spectrum of responses that include triggering additional information from the user, limiting the amount of damage that can be inflicted by reducing access to credit, initiating heightened monitoring, blocking suspicious activities and disabling accounts. These enable banks and card issuers to immediately trigger mitigations based on the risk of users or activity and to adapt quickly as threats change over time.

Because the system does not rely on securing the endpoints, banks can maintain better control of security and change the rules of the game at any time without having to retrain individual users or update endpoints. The logic, processes and analytics used by banks for authorizing transactions are not visible to, or reliant on, support from individual users, cards or payment-processing terminals. They are wholly under the control of the bank.

The ability to change the rules provides unfair advantage for the banks and the card system defenders—at least in the eyes of potential attackers. That's because they're never sure what defenses they're up against, what tripwires they need to avoid, whether they've been detected or when the defenses will change. Banks can adjust their system quickly without worrying about users or endpoint updates. This gives them the ability to adapt quickly, so they can mitigate the ever-changing methods used to perpetrate fraud.

These factors have enabled payment cards to thrive, despite being under constant attack and having suffered numerous compromises over the past two decades. Card payment security isn't perfect, but it has significant benefits that can be leveraged by the enterprise to protect its data.

Applying This Strategy to Enterprise Data Security

Traditional enterprise security strategies are based on a fortress model that prioritizes secure perimeters, hardened endpoints and over-reliance on user credentials. If the payment card security systems used the same fortress model, they would have lost the battle against malicious attackers long ago. Breaches, like those experienced by Target and other businesses, would have incurred long-term damage for everyone who uses, accepts or issues credit cards.

Fortunately, the payment card industry devised a better way. It realized it could address security and still provide users with flexibility by focusing on elements that are core to controlling risk and ensuring security, while avoiding strategies that limit agility.

As you'll see on the following pages, the methodologies that they deployed in creating a global payment capability can be adopted by enterprises that are seeking to deploy security to improve the protection of their data.

1. Monitor and control access in real time.

2. Enable analytics that provide insight on user behavior.

3. Use risk-driven mitigations that are endpoint-independent.

Monitor and Control Access in Real Time

1.

Securing enterprise data requires the ability to continuously monitor and intelligently control access. Solutions that help enterprises answer the following questions are essential:

- Do you know what is happening with your sensitive data assets?
- Do you know who, how, when and from where they're being accessed?
- Can you stop malicious access quickly?

Enterprises over-rely on authentication, which creates a serious weakness in enterprise defenses—mainly because external attackers only have to defeat one system to gain unlimited access to data assets. Additionally, authentication provides no deterrence or limitation on inside threats, which may include any party with access to your systems, such as partners, contractors and overseas development teams.

Protecting data doesn't mean having the greatest authentication, but rather having insight into how the data is being used and ensuring the data is only accessed appropriately. This method of controlling access to enterprise data is commonly referred to as adoptive access control. By monitoring users and enforcing real-time controls, the enterprise raises the bar for attackers by crippling the effectiveness of stolen credentials, compromised devices or automated bots.

Enable Analytics That Provide Insight on User Behavior

2.

Protecting enterprise data means being able to discern malicious activities and policy violations. It requires the use of data analytics that can actively assess ongoing activities and the behavior of users. Ideally, these analytics will use both historical data and real-time context to assess activities. Solutions that help enterprises answer the following questions are essential:

- Is this activity or event consistent with past activities of this user behavior, device and/or data?
- What do I know about this user's behavior, and does the activity make sense based on what others have done? (e.g., is it a new user or device? Do their cohorts or peers do similar things?)
- What users and activities are putting me at risk? What events, activities or characteristics have incurred this risk? Has the risk changed over time, and if so, why?

Analytics enable the enterprise to detect malicious and high-risk activity faster, while making it increasingly harder for attackers to get any foothold at all. The right analytics will automate the ingestion and processing of data in a way that exposes meaningful insight. These analytics allow the enterprise to understand how risks are changing over time and to use this information in both real-time access control decisions and proactive risk-management efforts, such as prioritizing which devices or identities need attention or intervention.

Use Risk-Driven Mitigations That Are Endpoint-Independent

3.

To maintain high levels of security, agility and data protection, the enterprise must maintain as much independence from the endpoint as possible.

By defining a security model that isn't wholly dependent on hardening or augmenting users' endpoints, the enterprise gains flexibility. There are too many different types of devices for the enterprise to keep up with, so that flexibility is essential. Furthermore, employees want the convenience of using any device, including the ones they own, to access enterprise email and other enterprise applications. To support these requirements, the enterprise needs to depend less on securing the endpoints.

The trade-off for relying less on the endpoint is that the enterprise security model must provide significantly more monitoring and security of data access. Resources that are sensitive and accessible, such as email, databases and SaaS applications, need to be actively monitored and protected using analytics-driven controls.

Ideally, the monitoring, analytics and controls are designed in a way that enables the enterprise to both understand and change their defenses readily without alerting attackers, updating endpoints or training users. The credit card industry has shown that not relying on securing endpoints can provide the flexibility to combat malicious activities.

Relying less on endpoint security will allow the enterprise to improve the quality of their access controls, adjust security more rapidly and protect their most important assets: data.

About the Solution From CA Technologies

CA Threat Analytics for PAM provides a continuous, intelligent monitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage—protecting data via the same behavior-analytics approach used by banks to defeat credit card fraud. Key features include:

Automated detection of attacks and risk

True, continuous monitoring uses automated analytics to quickly detect attacks, high-risk activities and breaches.

Advanced threat analytics

Machine-learning algorithms analyze historic and real-time activity to assess risk and trigger mitigations.

Integrated response and mitigation

The automatic triggering of mitigations, such as session recording and step-up authentication, closes the door on insiders and attackers.

By continuously analyzing user behavior, detecting malicious and high-risk activities and automatically triggering mitigating controls, CA Threat Analytics for PAM helps you prevent breaches, increase compliance and avoid costly penalties and brand damage.

Learn more at https://www.ca.com/us/products/ca-threat-analytics-for-privileged-access-manager.html

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-256229